ULIPOD
Uluslararası İlişkiler ve Politika Dergisi
Journal of International Relations and Politics
E-ISSN: 2792-0674
Ocak 2024 Cilt: 4 Sayı: 1

Makale Türü/ Article Type	Başvuru Tarihi/ Received	Kabul Tarihi/Accepted	Yayım Tarihi/Published Date
Araştırma Makalesi	26.04.2023	08.06.2023	10.01.2024

Hibrit Tehditler Kapsamında Türkiye'nin Kritik Altyapı Güvenliği: Petrol ve Doğalgaz Boru Hatları

Turkey's Critical Infrastructure Security in Hybrid Threats: Oil and Natural Gas Pipelines

Güngör Şahin*, Murat Emre EYGÜN**

Özet

Tarihin başından itibaren küresel ve bölgesel güç edinebilmek adına oldukça önemli yer edinen yeraltı zenginliklerinin dağıtımını ve korunmasını sağlayan kritik altyapı sistemleri mevcuttur. Türkiye'nin hibrit altyapı sistemleri ile petrol ve doğal gaz boru hatlarını kapsayan bu çalışmanın amacı, Türkiye'nin mevcut durumdaki var olan ve yakın gelecekte olası kurulacak olan kritik altyapı sistemlerinin, hibrit tehditlere karşı ne kadar hazır olup olmadığını, açığı kapatmak açısından neler yapılabileceğini ortaya koymaktır. Bu çalışma Türkiye'nin bölgesel güç odağında yerini sağlamlaştırması için kendi kritik altyapı sistemlerinin korunmasını sağlayabilmek açısından önemlidir. Esas olarak nitel araştırma yöntemini benimseyen bu çalışmada, doküman analizi, içerik analizi, grafik yorumlama ve yorumsamacılık gibi bilimsel araştırma yöntemlerinden yararlanılmıştır. Bu çalışma sonucunda elde edilen bulgular ise şöyledir: Günümüzde belirli bir refah seviyesine ulaşmış her devlet, kritik altyapıları, yaşam standartlarını belirleyecek en önemli başlık olarak görmektedir. Türkiye, iç güvenliğini sağlamlaştırmak adına kritik altyapı ve siber güvenlik konusunda geçmişten günümüze ciddi bir ilerleme kaydetmiş ve yol almış olsa da şu anda bulunduğu durumda günümüz dünyasının gereksinimlerine tam olarak ulaşamamış durumdadır.

Anahtar Kelimeler: Türkiye, Hibrit Tehdit, Kritik Altyapı, Petrol, Doğalgaz

Abstract

There are critical infrastructure systems that ensure the distribution and protection of underground riches, which have taken a very important place in order to gain global and regional power since the beginning of history. The aim of this study, which covers Turkiye's hybrid infrastructure systems and oil and natural gas pipelines, is to reveal how ready Turkiye's current and future critical infrastructure systems are to hybrid threats, and what can be done to close the gap. This study is important in terms of ensuring the protection of its own critical infrastructure systems in order for Turkiye to consolidate its place in the regional power focus. In this study, which mainly adopts the qualitative research method, scientific research methods such as document analysis, content analysis, graphic interpretation and hermeneutics were used. The findings obtained as a result of this study are as follows: Today, every state that has reached a certain level of welfare sees critical infrastructures as the most important topic that will determine their living standards. Although Turkiye has made significant progress and progressed from past to present in the field of critical infrastructure and cyber security in order to strengthen its internal security, it has not been able to fully meet the needs of today's world in its current state. For this reason, if Turkiye attempts a new supply center or a system project without providing the necessary competence, it may cause a disaster.

Keywords: Turkiye, Hybrid Thread, Critical Infrastructure, Oil, Natural Gas

* Doç.Dr. , Milli Savunma Üniversitesi, Atatürk Stratejik Araştırmalar ve Lisansüstü Eğitim Enstitüsü (ATASAREN), Strateji ve Güvenlik Araştırmaları Ana Bilim Dalı, gsahin@msu.edu.tr, ORCID: 0000-0001-6296-8568

** Yüksek Lisans Öğrencisi, Milli Savunma Üniversitesi, Atatürk Stratejik Araştırmalar ve Lisansüstü Eğitim Enstitüsü (ATASAREN), Strateji ve Güvenlik Araştırmaları Ana Bilim Dalı, Güvenlik Araştırmaları Yüksek Lisans Programı, meygun52@gmail.com, ORCID: 0000-0003-4048-1681

Atıf/Cite: Şahin, G. ve Eygün, M. E. (2024). "Hibrit Tehditler Kapsamında Türkiye'nin Kritik Altyapı Güvenliği: Petrol ve Doğalgaz Boru Hatları", Uluslararası İlişkiler ve Politika Dergisi, Cilt: 4, Sayı: 1, ss. 1-16

Giriş

Belki tarihin başından beri çok önemli bir pozisyonda olan ve coğrafyası o konumda olmasa dahi devletlerin politikalarını şekillendiren başlıca faktör yeraltı zenginlikleridir. Günümüz dünyasında da önemini ve küresel siyaseti şekillendirme konusunda etkisini kaybetmeyen yeraltı zenginlikleri, bu özelliğini Şubat 2022 itibariyle başlayan Rusya – Ukrayna savaşı sonrasında Avrupa tarafından Rusya'ya uygulanan ambargolara yönelik Rusya devlet başkanı Vladimir Putin'in Avrupa'ya ihraç ettikleri doğal gaz tedarikini durdurduğunu açıklaması sonucu Avrupa'nın arayışlarıyla kendini yeniden göstermiştir. 12 Ekim 2022 tarihinde Rusya devlet başkanı Vladimir Putin, Türkiye Cumhurbaşkanı Recep Tayyip Erdoğan ile yaptığı görüşmede, Türkiye'nin gaz tedariki konusunda güvenli bir güzergâh durumuna geldiğini ve Türkiye'de büyük bir ikmal merkezi kurma isteklerini dile getirdi. Bugüne kadar Avrupa'ya gaz aktarımı için kullanılan Kuzey Akım 1 Boru Hattı'nın devre dışı kaldığını hatırlatıp, bunun yerine Avrupa'ya aktardıkları gazın Türkiye üzerinden yapılabileceğini belirtti. "Bu durumda Türkiye'nin izlemesi gereken adımlar nelerdir? Türkiye böyle büyük bir ikmal merkezi kurulması ihtimalinde bu merkezin altyapı sistemlerinde güvenliğe verilmesi gereken önem neden mühimdir?" gibi sorulara cevap arayan bu çalışmada aynı zamanda "Hibrit tehdit nedir? Kritik altyapı nedir? Altyapı güvenliği nedir? Türkiye Petrol ve Doğalgaz Boru Hatları hangi hatlardır, nerededir? Türkiye'de Kritik Enerji Altyapı Unsurları Güvenliğinin Sorunları, Tehditleri ve Riskleri nelerdir? Türkiye'nin Ulusal Güvenlik Strateji Belgesinde kritik altyapıların korunmasına dair açıklanan girişimler nelerdir?" gibi sorulara da cevap aranacak ve bulgulara yer verilecektir.

Bu çalışmanın konusu, hibrit tehditler kapsamında Türkiye'nin kritik altyapı güvenliğinde petrol ve doğal gaz boru hatlarının güvenliğidir. Kritik altyapı tesislerine odaklanılacak, Türkiye adına petrol ve doğalgaz altyapı tesislerine bakılacak ve bu tesislerin güvenlik düzeyleri göz önüne serilecektir. Araştırmada bu tesislerin güvenlikleri ışığında Türkiye'nin altyapı güvenliği incelenecektir. Bu çalışmanın amacı özellikle enerji kaynaklarının üretimi ve dağıtımı için önemli bir konu olan kritik altyapı tesislerinin güvenliğinin Türkiye'deki yansımalarına bakmaktır. Güvenlik çalışmaları ışığında Türkiye'nin olası altyapı anlaşmaları sonucunda kuracağı merkez ve altyapı tesislerinin incelenmesini temel alan bu çalışma Rusya – Türkiye olası ikmal merkezi kurulumu gerçekleşmesi dâhilinde önem kazanacaktır. Çalışmanın ana hipotezi; Türkiye'nin mevcut durumdaki var olan ve yakın gelecekte olası kurulacak olan kritik altyapılarının, hibrit tehditlere karşı tam olarak hazır olmadığı ve bu açığın kapatılması adına, bugüne kadar neler yapıldığı ve bugünden sonra neler yapılabileceğidir.

Çalışmamıza özgün değer katan en önemli husus, bu çalışmanın, Türkiye – Rusya olası ikmal merkezi anlaşmasının güncel bir olay olması ve bu ihtimal dâhilinde kurulacak olan kritik altyapı tesisinin Türkiye adına enerji konusunda bir çığır açması olacağı düşüncesidir. Şimdiye kadar yapılan çalışmalarda, kritik altyapı tesisleri incelenmiş, siber terörizme karşı izlenmesi gereken adımlar incelenmiştir. Bu çalışma henüz kurulmamış bir altyapı tesisini ele alması ve bu tesisin nasıl olması gerektiğini incelemesi bakımından özgün bir değere sahiptir.

Çalışmanın kavramsal çerçevesini kritik altyapı sistemlerinin korunması, siber tehditlere ve fiziki saldırı ya da olumsuz olaylara karşı durumları, açıklıkları ve bu konuda Türkiye'nin güncel güvenlik durumu oluşturmaktadır. Bu çalışmanın amacına ulaşabilmesi adına, nitel araştırma metodolojisi benimsenecek, literatür taraması, doküman analizi, içerik analizi, grafik yorumlama ve yorumsamacılık gibi bilimsel araştırma yöntemlerinden

yararlanılacaktır. Var olan kamu tesislerinin incelenmesi ve bunların güvenliğine odaklanılmasından dolayı resmi kurumlardan alınacak olan bilgilerin en doğru bilgiler olacağı değerlendirilmiştir. Bu sebeple doküman analizleri yapılacaktır. Araştırmanın yukarıda belirtilen adımları tamamlandıktan sonra elde edilen bilgiler ışığında Türkiye'nin var olan kritik altyapı tesislerinin güvenliği ve olası ikmal merkezi için kuracağı altyapı tesisinin güvenliğinin nasıl sağlanması gerektiği yorumlanacaktır.

Bu konu temelinde var olan çalışmalarda ilk olarak kritik altyapı kavramı, altyapı tesisleri ve bunların korunması incelenmiştir (Ünver M. vd., 2011). Bu çalışmada kritik altyapı kavramının tanımı, kapsamı ve bu kapsam altında düzenleyici çerçeveler ülke ve uluslararası örgütler temel alınarak incelenmiş ve kritik altyapı korunması hususunda yapılan çalışmalar ülke temelli kategorize edilmiştir. İkinci olarak Türkiye'de siber terörizme karşı bilişim teknolojilerinin kullanımına yönelik çalışmalar yapılmıştır (Doğan A., 2021). Bahsi geçen çalışmada terör ve terörizm kavramı üzerine durulmuş, siber terörizm ve bu terör çeşidine karşı bilişim teknolojilerinin kullanılması temel alınmıştır. Bu yaklaşımlar çalışmamıza katkı vermekle beraber tam olarak açıklanması istenen konuya dair net bir ışık tutmamaktadır.

Çalışma dört bölümden oluşacaktır. Birinci bölümde çalışmaya teorik bir çerçeve oluşturabilmek adına "Hibrit Tehdit" ve "Kritik Altyapı" kavramları ele alınacaktır. Bu kavramların tanımı ve kritik altyapı tesislerine yönelik tehditler ile bahsi geçen kavramların iç güvenlik ile bağdaştırılması işlenecektir. Kritik Altyapı başlığı altında Dünya'da kritik altyapı kavramına odaklanılacaktır. Avustralya, Almanya, Kanada, Hollanda, Birleşik Krallık, Amerika Birleşik Devletleri gibi ülkelerin kritik altyapı kavramına yaklaşımları ve tanımlamalarına yer verilecektir. Çalışmanın ikinci bölümünde "Türkiye Petrol ve Doğalgaz Boru Hatları" incelenecek ve T.C. Enerji ve Tabii Kaynaklar Bakanlığı'nın yayınladığı bilgiler temel alınarak bu hatların tanıtımı yapılacak. Çalışmanın üçüncü bölümünde "Türkiye'de Kritik Enerji Altyapı Unsurları Güvenliğinin Sorunları, Tehditler ve Riskler"e odaklanılacaktır. Çalışmanın son bölümünde ise "Kritik Altyapılar ve Siber Güvenlik" başlığı adı altında Türkiye'nin "Ulusal Siber Güvenlik Stratejileri ve Eylem Planı Hazırlıkları" ele alınacaktır. Bu belgede kritik altyapı tesislerinin korunması adına neler ele alındığına odaklanılacaktır. Çalışmanın sonuç bölümünde ise elde edilen bilgiler ışığında boru hatlarının güvenliğinin analizi yapılacak, bu bölümde Türkiye'nin elinde hazır olan ve gelecekte olması muhtemel yeni kritik altyapı tesislerinin korunması için neler yapması gerektiği ele alınıp tartışılacaktır.

1. Kavramsal Çerçeve

Çalışmada incelenecek olan başlıca iki kavram söz konusudur. Bunlardan birincisi "Hibrit Tehdit" kavramıdır. Bu alt başlık altında "Hibrit" ve "Hibrit Savaş" kelimesinin sözcük anlamı incelenecek ve devamında hibrit savaş kelimesinin literatüre girişinin kim tarafından ve ne zaman sağlandığı incelenecektir. Hibrit savaş/tehdit kavramı üzerine inceleme yapıldıktan sonra ikinci başlık olarak "Kritik Altyapı" kavramı incelenecektir. Bu kavramın sözcük anlamı incelendikten sonra, bu anlamların ülkeden ülkeye ya da kurum ve kuruluşlar arasındaki tanım farklılığı ele alınıp çalışmanın temeli oluşturulacaktır.

1.1. Hibrit Tehdit

Hibrit kelimesinin Türkçe anlamı göz önüne alındığında, karışık kuvvetlerin veya iki farklı kuvvetin birleşimini içerir. Bu bakımdan hibrit savaş, en az iki farklı askeri stratejiyi veya savaş türünü içeren bir savaş türüdür (Erol ve Oğuz, 2015: 263). Hibrit savaş, siyasi savaş, fiziksel savaş, siber savaş, propaganda, sahte haberler, aldatma, ekonomik

yaptırımlar, terörizm, diplomasi ve dış seçim müdahalesi gibi teknikleri kullanan askeri bir stratejidir. Hibrit savaş, ulusal gücün ve mücadelenin tüm unsurlarını içeren, devam eden ve sınırsız bir savaştır. Kavramı ilk olarak açıklayan yazarlardan olan Frank Hoffman da hibrit savaşı en genel haliyle, "devlet çatışmasının ölümcüllüğü ile düzensiz savaşın fanatikliği ve uzun süren coşkusunun harmanlanması" olarak tanımlamıştır (Hoffman, 2007). Hibrit harp, geleneksel harp/askeri harp ile geleneksel gerilla/kontrgerilla harbi ve yöntemlerinin birleşmesi sonucu ortaya çıkmış yeni bir konvansiyonel olmayan savaş şeklidir. Sadece savaşla ilgili araçlar değil, savaşla ilgili olmayan araç ve yöntemler de vardır (Toptaş, 2015: 5).

Hibrit savaş kavramı ilk olarak 8 Eylül 2005'te Virginia'daki Deniz Güçleri Forumunda James N. Mattis tarafından kullanıldı (Mattis & Hoffman, 2005). Söz konusu kavram, 2006 yılı Lübnan krizini ve Hizbullah-İsrail çatışmasını analiz eden Frank Hoffman tarafından geliştirildi. Frank Hoffman, 2007 yılında hibrit savaş terimini literatüre kattı. Hoffman'a göre devletler arasındaki klasik savaş yerini sivil, askeri, örgütlü şiddet, terör, suç ve savaş arasında net bir ayrımın olmadığı melez bir savaşa bırakmıştır. Hoffman, hibrit savaşı, konvansiyonel güçleri, stratejik planlama ve koordinasyonu içeren bir askeri strateji ile şiddet, zorlama ve provokasyonu içeren terörist faaliyetleri olarak tanımlamıştır (Hoffman, 2007: 29).

Hibrit savaş kavramı, Rusya Genelkurmay Başkanı Valery Gerasimov'un "Geleceğin Bilimsel Değerleri" başlıklı makalesiyle ivme kazandı. Gerasimov'un doktrini ya da anlamsız savaş olarak da bilinen bu süreçte Gerasimov, makalesinde, savaş ve barış arasındaki çizginin giderek güçleştiği, siyasi ve askeri zaferlerin kazanıldığı 21.yüzyılda; askeri olmayanın rolünün arttığını ve klasik ordunun rolünün barış zamanına kadar uzandığını iddia etmektedir (Gerasimov, 2013). Hizbullah'ın 2006 yılı Lübnan krizinde İsrail'e karşı stratejisi, 2008 yılı Beş Gün Savaşı sırasında Rusya'nın Gürcistan'a karşı stratejisi ve 2014 yılında Kırım krizinde Rusya'nın Ukrayna'ya karşı stratejisi hibrit savaşın son örnekleri olarak ifade edilebilir.

1.2. Kritik Altyapı

Kritik altyapılar dediğimiz sistemler, insanların topluca yaşadığı bir ülke veya toprakta, vatandaşların hayat kalitesine ve refahına dayanak olan sistemlerdir. Özellikle de bu vatandaşların ülkesindeki, toprağındaki toplu bilinç ve milli kimlikleri sanayi ve üretim üzerine şekillendirilmişse, bu millet, altyapıların önemi ve değerini daha çok anlayacak ve daha çok vurgulayacaktır. Bahsi geçen altyapı sistemlerinin "kritik" düzeyleri ise, bu sistemlerin bir şekilde devre dışı kalması ya da saldırıya uğraması sonucunda var olan düzenin ne derece aksayacağına bağlı olarak doğru orantılı şekilde değişir.

Kritik altyapının tanımına bakıldığı zaman, bu sistemlere ve güvenliklerine yönelik ilk düşünceler Amerika Birleşik Devletleri (ABD)'nde görülmüştür. ABD'de 1996 yılında oluşturulmuş olan kanun hükmünde kararname (Clinton, 1996: 1) ve 1997 yılında hazırlanan rapora göre, kritik altyapılar, askeri, ekonomik, siyasi vb. yönlerden bahsi geçen ülke adına hayati öneme sahip olan tesisler olarak kabul edilmiştir. ABD, o yıllarda "kritik altyapı" kavramını, çalışmaması veya çökmesi durumunda ulusal savunma ve ekonomik güvenliğini zayıflatma etkisine sahip olan yerler olarak ifade etmiştir (Karanacak, 2011; US PCCIP, 1998).

1996 tarihli Başkan Clinton'ın Kritik Altyapıların Korunmasında Başkanlık Komisyonu Kurulması Kararnamesi'nde altyapı kavramı; *"Birbirine bağlı ağ yapıları, belirlenmiş endüstrileri içeren sistemler, insanlar ve süreçleri içeren kurumlar, ülkenin savunması*

ve ekonomisinin güvenliği için toplumun tamamı ile devletin her seviyede sorunsuz işleyişi için gerekli olan güvenilir ürün ve hizmet akışını sağlayan dağıtım yetenekleridir" (Clinton, 1996: 1) olarak tanımlanmıştır. 11 Eylül 2001 terör saldırısı sonrasında "Anayurt Güvenliği Ofisi ve Konseyi'min kurulmasına ilişkin Kararname" içinde kritik altyapılar; insanların kullanımı ve tüketimi için tarımdan sanayiye her türlü gerekli sistem ve güvenlik, enerji, bilgi sistemleri gibi her türlü sistemler olarak sayılmıştır (Moteff & Parfomak, 1988: 3).

Daha sonrasında 2001 yılı Yurtseverlik Yasası ve ardına 2002 yılında Anayurt Bakanlığı ve Başkanlık tarafından da bir tanımlanmaya tabi tutulan kritik altyapılar 2003 yılında oluşturulmuş olan *"Kritik Altyapı ve Temel Varlıkların Korunması için Ulusal Stratejisi"* belgesinde de benzer tanımlamalar ve vurgular yapılmıştır (Moteff & Parfomak, 2003: 6). ABD adına bakıldığında, kullandığı kritik altyapı kavramları seneler içerisinde gelişse ve değişse de, yıllar içerisinde "kritiklik" ölçüsünün değişimine göre bu konuya verilen önemin arttığı söylenebilir.

Avrupa'daki kritik altyapıların tartışılması 11 Eylül terör saldırıları sonrasında gelişmiştir ve bu durum özellikle bu sistemlerle ilgili ülkeler arasında işbirliğini arttırmıştır. Özellikle, 2004 yılında meydana gelen Madrid'in tren ağlarına yönelik saldırı ve ardına bir yıl sonra Londra metro istasyonuna yapılan terör saldırıları bu konu üzerine dikkatleri daha çok çekmiştir. Avrupa Komisyonu tarafından 2004 yılında hazırlanan *"Terörle Mücadele için Kritik Altyapı Korunması"* başlıklı belgede kritik altyapılar *"kesintiye uğraması veya yok edilmesi durumunda üyesi olan devletlerin vatandaşlarının sağlığı, emniyeti, güvenliği ve ekonomik refahı veya hükümetlerin etkin işleyişi üzerinde olumsuz etkisi olacak olan fiziksel ve bilgi teknolojileri tesisleri, ağları ve hizmetler ve varlıkları"* olarak tanımlanmıştır (Ak, 2019: 44; EU COM702(F1), 2004: 4).

Birleşmiş Milletler (BM) Güvenlik Konseyi de 11 Eylül saldırıları sonrasında ülkeleri kritik altyapılarını korumaya yönelik önlemler almaya çağırmış ve bu tür saldırılara verilecek cevabın hız konusunda önemli bir faktör olduğunu belirtmiştir (UN Security Council, 2001; UN Security Council, 2004). Aynı şekilde BM Güvenlik Konseyi, 2017 senesinde *"Terörist Saldırılara Karşı Fiziki Altyapıların Korunması"*(UN CTED, 2017) ve 2018 senesinde ise *"Terörist Saldırılara Karşı Kritik Altyapının Korunması"*(UN CTED & UNOCT, 2018) isimle yayınladığı raporlar ile de önlem almaya tekrardan dikkat çekmiş ve bu önlemlerin arttırılmasına çalışmıştır.

Türkiye'de ise kritik altyapı kavramı ve faaliyetleri Afet ve Acil Durum Yönetimi Başkanlığı (AFAD) tarafından tanımlanmıştır. AFAD'ın kritik altyapı tanımı "2014 – 2023 Kritik Altyapıların Korunması Yol Haritası Belgesi"nde görülmektedir. *"Kritik altyapılar; İşlevini kısmen veya tamamen yerine getiremediğinde çevrenin, toplumsal düzenin ve kamu hizmetlerinin yürütülmesinin olumsuz etkilenmesi neticesinde, vatandaşların sağlık, güvenlik ve ekonomisi üzerinde ciddi etkiler oluşturacak ağ, varlık, sistem ve yapıların bütünüdür"*(AFAD, 2014a: 4). Bu tanıma benzer bir tanım da yine aynı şekilde AFAD'ın *"Açıklamalı Afet Yönetimi Terimleri Sözlüğü"*nde yer almaktadır (AFAD, 2014b: 106).

Kritik altyapı kavramı bütün dünyada iki kelimenin ayrı şekilde incelenmesi ve ardına birleştirilmesi şeklinde tanımlanmaktadır. Tablo 1'de birtakım ülkelerin kritik altyapı kavramının tanımları görülmektedir.

Tablo 1. Kritik Altyapının Ülke Tanımları

Avustralya	*"Kritik altyapı, yok edilmesi, bozulması veya uzun süre kullanılamaz hale getirilmesi durumunda ülkenin sosyal veya ekonomik refahını önemli ölçüde etkileyecek veya Avustralya'nın ulusal savunma yapma ve ulusal güvenliği sağlama yeteneğini etkileyecek fiziksel tesisler, tedarik zincirleri, bilgi teknolojileri ve iletişim ağları olarak tanımlanır."* (Australian National Security, 2022)
Kanada	*"Kanada'nın kritik altyapısı, kesintiye uğraması veya yok edilmesi durumunda Kanadalıların sağlığı, güvenliği ve ekonomik refahı veya Kanada'daki hükümetlerin etkin işleyişi üzerinde ciddi bir etkisi olacak fiziksel ve bilgi teknolojisi tesisleri, ağları, hizmetleri ve varlıklarından oluşuyor."* (Canada's Critical Infrastructure, 2022)
Almanya	*"Kritik altyapılar, başarısızlığı veya değer düşüklüğü sürekli tedarik kıtlığına, kamu düzeninde önemli aksamalara veya diğer dramatik sonuçlara neden olacak toplum için büyük öneme sahip kuruluşlar ve tesislerdir."* (Germany Federal Office, 2004)
Hollanda	*"Kritik altyapı, bozulma veya başarısızlık durumunda büyük sosyal rahatsızlığa neden olabilecek ürünleri, hizmetleri ve beraberindeki süreçleri ifade eder. Bu muazzam kayıplar ve ciddi ekonomik zararlar şeklinde olabilir…"* (Netherlands Ministry of Justice and Security, 2018)
Birleşik Krallık	*"Kritik Ulusal Altyapı, İngiltere'nin ekonomik, politik ve sosyal yaşamını destekleyen varlıkları, hizmetleri ve sistemleri içerir; önemi, kaybın şu şekilde olabileceği şekildedir: 1) büyük ölçekli can kaybına neden olmak. 2) ulusal ekonomi üzerinde ciddi bir etkiye sahip olmak. 3) İngiltere'nin ekonomik, politik ve sosyal yaşamını destekleyen diğer ciddi sosyal sonuçları vardır. 4) Ulusal hükümeti endişelendirir. "* (United Kingdom Home Office Security, 2012)

Kaynak: Gordon & Dion, 2018: 4

Bir önceki başlıkta ve yukarıda Tablo 1'de de belirtildiği gibi her ülke kritik altyapı kavramının tanımını yapmıştır. Bu tanımlar yapılırken halkın refah düzeyi, yaşamın başlıca gereksinimleri temel alınmıştır. Kritik altyapıların devletler ve milletler için önemi ortaya koyulmuştur. Sonuç olarak; ülke, coğrafya, bölge, kurum ya da kuruluş farklılıklarına rağmen kritik altyapıların tanımlarında ortak olan nokta, kritik altyapı sistemlerinin, vatandaşların hayatının düzenini bozan, devletleri zor durumda bırakan, hizmetleri ve refah seviyesini bizzat belirleyen sistemler olmasıdır.

2. Türkiye Petrol ve Doğalgaz Boru Hatları

Bulunduğu coğrafyadan kaynaklı olarak Türkiye, Kafkasya bölgesinden, Orta Doğu bölgesinden, Avrupa'ya yönelik transit boru hatlarına sahip olduğu gibi aynı sayıda olmasa da kendi sınırları içerisinde de petrol ve doğalgaz boru hatlarına da sahiptir. Türkiye'nin petrol hatları sayısı dört adettir. Bu hatlardan iki tanesi ulusal hatlardır, diğer iki hat ise yurtdışından gelen transit hatlardır.

Ulusal hatlar "Ceyhan – Kırıkkale" ve "Batman – Dörtyol" hatlarıdır. Bu hatlardan ilk kurulanı Türkiye'nin de ilk ham petrol boru hattı olan Batman – Dörtyol Ham Petrol Boru Hattı'dır. 1967 tarihinde işletmeye açılmıştır ve mülkiyeti 1984 tarihinde Boru Hatları İle Petrol Taşıma Anonim Şirketi'ne (BOTAŞ) devredilmiştir (BOTAŞ, 2023). Türkiye'nin ikinci ulusal ham petrol boru hattı Ceyhan – Kırıkkale Ham Petrol Boru, inşaatına 1983

yılında başlanan ve 1986 yılında bitirilen Adana ilinin Yumurtalık ilçesinden başlayıp Kırıkkale iline uzanan 457 km uzunluğunda olan boru hattıdır. Yıllık kapasitesi 7.2 milyon tondur (BOTAŞ, 2023).

Transit rolüyle karşımıza çıkan ilk petrol boru hattı ise Kerkük – Yumurtalık Boru Hattı ismi de olan Irak – Türkiye Ham Petrol Boru Hattı'dır. 1973 senesinde Irak ile Türkiye arasında imzalanan "Ham Petrol Boru Hattı Anlaşması" çerçevesinde, 986 kilometre uzunluğunda inşa edilen hat, 1976 senesinde işletmeye açılmıştır. 19 Eylül 2020 tarihinde var olan anlaşmanın 15 yıl boyunca uzatılmasına yönelik anlaşma imzalanmıştır. Boru hattının Türkiye topraklarındaki sahibi ve işletim hakkı olan kurum BOTAŞ'tır (T.C. Enerji ve Tabii Kaynaklar Bakanlığı, 2023a).

Transit olarak geçen ikinci petrol boru hattımız ise Bakü-Tiflis-Ceyhan Ana İhraç Ham Petrol Boru Hattı (BTC). Hazar bölgesinden gelen petrolü Azerbaycan'dan, Gürcistan'a oradan da önce Erzurum'a sonra Ceyhan'a uzanan bu hat Ceyhan'dan Akdeniz üzerinden dünya pazarlarına sunulmaktadır. 1999 tarihinde Azerbaycan, Gürcistan, Türkiye arasında imzalanan Hükümetlerarası Anlaşma ile bu anlaşmanın eki olan Evsahibi Hükümet Anlaşması 2000 tarihinde imzalanmıştır. BTC boru hattının toplam uzunluğu 1768 km'dir. Bu uzunluğun 249 km'si Gürcistan, 443 km'si Azerbaycan ve 1076 km'si ise Türkiye üzerinden geçmektedir. Hattın Türkiye topraklarında yer alan kısmını BOTAŞ işletmektedir (T.C. Enerji ve Tabii Kaynaklar Bakanlığı, 2023a).

Bahsedilen hatlar, ulusal ve transit petrol hatlarıydı. Türkiye üzerinden geçen ya da Türkiye içinde bulunan diğer hatlar da doğalgaz boru hatlarıdır. T.C. Enerji ve Tabii Kaynaklar Bakanlığı'nın sitesindeki verilere göre Türkiye üzerinden geçen ya da Türkiye içinde bulunan mevut doğalgaz boru hattı sayısı 7 adettir. Bunlar; Rusya – Türkiye Doğal Gaz Boru Hattı (Batı Hattı), Mavi Akım Gaz Boru Hattı, Doğu Anadolu Doğal Gaz Ana İletim Hattı (İran – Türkiye), Bakü-Tiflis-Erzurum Doğal Gaz Boru Hattı (BTE), Türkiye-Yunanistan Doğal Gaz Enterkonneksiyonu (ITG), Trans-Anadolu Doğal Gaz Boru Hattı (TANAP), TürkAkım Gaz Boru Hattıdır. Rusya – Türkiye Doğalgaz Boru Hattı, Sovyetler Birliği ve Türkiye arasında 1984 tarihinde imzalanan anlaşma ile kararlaştırılmıştır. 1985 yılında inşası başlayıp 1987 yılında da işleve başlamıştır. Bu hat 845 km uzunluğuna sahiptir. Bu hattın işletmesini de tıpkı diğerlerinde olduğu gibi BOTAŞ üstlenmiştir (T.C. Enerji ve Tabii Kaynaklar Bakanlığı, 2023b).

Ele alınacak ikinci hat Mavi Akım Gaz Boru Hattı'dır. 1997 yılında BOTAŞ ve Gazprom Export şirketleri tarafından 25 yıllık Doğalgaz Alım-Satım anlaşması yapılmıştır. 2003 yılında işletmeye alınmış, 2005 yılında ise resmi olarak açılmıştır. Toplam 1569 km uzunluğundadır. Bu uzunluğun 678 km'si Rusya topraklarında, 390 km'si Karadeniz'de, 501 km'si ise Türkiye topraklarındadır (T.C. Enerji ve Tabii Kaynaklar Bakanlığı, 2023b). Bu hatlar dışında oldukça önem arz eden diğer doğalgaz boru hatları da vardır. Bu çalışma adına önem arz eden nokta ise bu hatların tanıtımından çok güvenliği olacaktır.

3. Türkiye'de Kritik Enerji Altyapı Güvenlik Sorunları, Tehditler ve Riskler

Petrol ve doğalgaz gibi enerji kaynaklarının bir yerden diğer bir yere naklini sağlayan enerji nakil hatları, ulusaldan uluslararasına doğru birbiriyle bütünleşmiş durumda olan hatlardır. Bu özelliklerinden ötürü bu hatların birinde ya da bir noktasında problem ortaya çıkması halinde bütün sistem bu problemden etkilenmektedir. Bu problemler; fiziki ateşli saldırı, sabotaj, hırsızlık, ihmal ya da kazalar, afetler, sızıntılar ve fiziki ya da siber alanda yapılan terör saldırıları vb. olarak sayılabilir. Bu sayılan problemlerin ortaya çıkması halinde bütün enerji akışı durabilmekte ve tonlarca enerji kaybına da sebep olabilmektedir.

Türkiye'de yukarıda sayılan problemlerin yaşanmaması için çalışan ve bu ihtimalleri en aza düşürmek için uğraş veren kurum ve kuruluşlar birçok güvenlik önlemi almaktadırlar. Özellikle son yıllar temel alındığı zaman bu konular enerji arzı probleminden çıkıp savunma sanayi alanına girdiğinden ötürü, savunma sanayi şirketleri birçok sistem geliştirmekte ve altyapı güvenlik riskini en aşağı kademeye çekmeye çalışmaktadır. Türkiye günümüzde bir tür enerji köprüsü görevi görmekte ve uluslararası topraklara doğru bir boru hattı genişletmektedir. Bu hatların uzunluğu ne kadar artarsa aslında var olan tehditler ve güvenliği sağlama zorluğu da o denli artacaktır.

Türkiye'nin gerek coğrafi gerekse de politik anlamda en başta gelen problemi de terör örgütleridir ve bunlarla verilen mücadelede de kritik altyapıların önemi yıllar geçtikçe anlaşılmaya başlanmıştır. Terörizm, Türkiye adına sadece ülke sınırlarını değil bu tip hayati sistemleri de vurmuştur ve tehdit etmiştir. 2015 senesinde "Türkiye – İran Doğalgaz Boru Hattı"na yapılan saldırı bunu açık bir şekilde göstermiştir. 2014 yılı verilerine göre Türkiye'nin doğalgaz ihtiyacının %18'ini karşılayan bu hatta yapılan saldırı sonucunda gaz akışı bir hafta durmuştu. Olayın bir gün sonrasında ise Kerkük – Yumurtalık Petrol Boru Hattı'na yönelik bir saldırı olmuş ve bu saldırı sonucunda Irak'ın zararının 250 milyon dolar olduğu açıklanmıştı (Erkal, 2018: 66). Bu saldırıların hemen bir ay sonrasında bu sefer de Bakü – Tiflis – Erzurum Doğalgaz Boru Hattı'na yönelik bir saldırı meydana gelmişti. Az önceki gibi yine 2014 yılı verilerine göre bu hattın da Türkiye'nin doğalgaz ihtiyacının %12,3'lük kısmının bu hat üzerinden karşılandığı bildirilmiştir (Erkal, 2018: 66). Bir diğer saldırı çeşidi de siber saldırılardır. 2017 yılında Kerkük – Yumurtalık Hattı hedef alınarak bir saldırı gerçekleştirilmişti (Erkal, 2018: 67). Bu saldırının kaynağı olarak ise Enerji ve Tabi Kaynaklar Bakanlığı, ABD olarak açıkladı.

Enerji güvenliği konusu politik gözle incelendiği zaman, devletlerin birçok yönden risk altında olduğu bir alan haline gelmiştir. Bu sebeple gerek Türkiye'de gerekse de diğer ülkelerde bu konunun üzerine odaklanılma hali daha da artmıştır. Enerji arz güvenliğinin sağlanmasından ötürü altyapı tesislerinin faaliyet göstermemesi ülkelerin gelecekteki enerji vizyonlarını tehlikeye sokup tartışmaya açık bir duruma getirmektedir. Gerçekleşen saldırılar ile meydana gelen çevresel sıkıntılar, mali kayıplar ve tahribatlar ülke ekonomisine darbe indirip kalkınmayı olumsuz bir şekilde etkilemektedir. Buna karşılık dışarıdan alınan enerjiye bağımlı olan Türkiye adına enerji şirketlerinin millileştirilmemesi de bir tehdit ve risk oluşturmaktadır. Türkiye'nin bu saldırıları önlemek ve tehditleri en aza indirebilmesi için bir güvenlik kalkanı oluşturması gerekmektedir.

Hâlihazırda var olan ve önümüzdeki süreç ya da yıllarda inşa edilmesi olası ya da planlanan her enerji hattı için Türkiye, transit bir ülke olarak yerini bulacaktır. Bu durum elbette Türkiye ve karar alıcı diğer devletlerin arasındaki ekonomik ve politik işbirliğine bağlıdır. Bu olasılıklar dâhilinde Türkiye adına yapılması gereken, anlaşmaya çalıştığı ülkenin güvenini kazanmak ve kendi elini güçlendirmek adına bu var olan tesislerin güvenliğini sağlamak ve hatlardan geçecek olan malzemelerin, hedef bölgeye sıkıntısız bir şekilde iletilmesini sağlamaktır. Bu hatların güvenliğini sağlaması Türkiye adına zenginlik ve güç getirisi sağlarken aynı zamanda bulunduğu coğrafyada da güvenlik hassasiyetini arttıracaktır.

Türkiye bulunduğu coğrafya açısından gerek terör sorunu gerekse de Orta Doğu ve Kafkasya başta olmak üzere bölgedeki istikrarsızlık ve karışıklılık Türkiye adına güvenliği sağlamayı zorlaştıran etmenlerdir. Sabotaj, Vandalizm ve hırsızlık gibi olaylar da bu tehdidi arttıran bir diğer önemli konulardandır. Dolayısıyla bu hatların inşasından da daha önem arz eden konu bu hatlarda sağlanan ve sağlanacak olan güvenlik tedbirleridir.

1990'lı yıllardan bu zamana kadar Türkiye'nin boru hatlarına yönelik olarak yaklaşık 170 adet saldırı veya saldırı girişimi olmuştur. Bu saldırıların bir kısmının başta PKK olmak üzere birtakım terör örgütleri tarafından yapıldığı düşünülmektedir. Saldırılan hatların çoğunluğunun güney hatları olması da bu düşünceye katkı sağlayan bir detaydır. Bu saldırılar dışında pek çok hırsızlık ve vandallık da görülmüştür. Ancak Türkiye, çok büyük sıkıntılarla karşılaşmasa bile, bu sistemlere yönelik saldırıların korunmasına yönelik gereken adımları atmasına karşın bu güvenlik öncelikli politikalarını daha da ileri taşımalıdır. Türkiye gerek bulunduğu konum olarak Asya ve Avrupa arasında bağlayıcı durumunda olması gerekse de güncel küresel siyasetteki konjonktür sebebiyle Avrupa'ya bir enerji taşıma noktasında öne çıkmış ve potansiyel sahibi bir ülke durumundadır.

Türkiye'de boru hatları ve kritik altyapıların korunmasına yönelik sorumlu kuruluş BOTAŞ'tır. Bu tip tesislerin her türlü siber ve fiziki saldırılara açık olduğu daha önce belirtildi. Bu sistemlerin bir ülkenin refah seviyesini belirlediği gibi politik anlamda da devletin gücünü belirlediğini de belirtmek gerekiyor. Bu sebeple bu tesislerin güvenliği ve korunması konusunda BOTAŞ ile beraber eş zamanlı olarak kolluk kuvvetleri ve İHA'lar da dâhil olmak üzere savunma sanayii ürünleri kullanılmaktadır.

Türkiye'de altyapıların güvenliğine ilişkin ABD merkezli Honeywell şirketi öne çıkmaktadır. Honeywell 1992 yılından beri Türkiye'de çeşitli sistemlerde güvenliği sağlamak ve bu sistemleri daha verimli hale getirmek için birtakım çalışmalar yapmaktadır. Türkiye bu sistemlerin korunması için Honeywell şirketinin geliştirdiği işletim sistemlerini, teknolojileri, ekipmanları ve yazılımları kullanmaktadır. Türkiye dışa bağlılıktan uzaklaşmak ve millileşmek amacıyla 2016 yılında Aselsan ve Havelsan savunma şirketleri ile "Savunma Sanayii Başkanlığı ile Boru Hatları Güvenliği Projesi" sözleşmesini imzalamış ve iki şirketin ortaklığıyla beraber boru hatları için güvenlik sağlayan savunma sistemleri geliştirmeyi planlamıştır. 2016'da yapılan sözleşme dâhilinde 28 Ekim 2018 tarihinde Aselsan ve Havelsan bir araya gelerek, Silopi'de saha uygulamaları için "Petrol ve Doğalgaz Hatlarının Güvenliği Projesi" anlaşması imzalamıştır. Proje dâhilinde kritik tesisler hırsızlık, terör, sabotaj gibi saldırılara karşı yerli İHA ve kapalı devre kamera alt sistemleri ile 7/24 koruma altındadır (HAVELSAN, 2023; BOTAŞ, 2018).

4. Kritik Altyapılar, Siber Güvenlik ve Türkiye'nin Ulusal Siber Güvenlik Stratejileri

Siber alan, iletişim ağlarının, veri tabanı ve bilgi kaynaklarının toplanıp geniş kapsamlı, karmaşık ve çeşitli, elektronik nitelikli karşılıklı iletişim kütlesi oluşturmasını ifade etmektedir (Collins, 2017: 363). Marshall McLuhan, internetin, dünyayı küresel bir köye çevirdiğini söylemiştir. Dünyanın küresel köye benzetilmesine sebep olan durum hiç şüphesiz internetin ülke sınırlarını etkisiz bırakmasıdır. İnsanlar internet sayesinde birkaç saniye içerisinde dünyanın her tarafında meydana gelen olaylarla etkileşim hali içinde olabiliyor. İnternet ağının dünyanın her yerinde ve neredeyse herkesin ulaşımında olması tabi bu mecrayı bir güvenlik sorunu haline de getirmiştir. Bu güvenlik sorunlarının başında da siber saldırılar gelir.

Siber saldırı; savunma ya da saldırı amacına bakılmaksızın, insanların yaralanmasına ya da ölmesine, nesnelerin yok olmasına ya da zarar görmesine sebep olan siber ortamda gerçekleşen eylemler olarak tanımlanmaktadır (Schmitt, 2013: 92). Bir diğer tanıma göre, siber saldırı; hedeflenen bilgisayar sistemleri ve ağlarını (ve tabi bu sistemlerde bulunan mesaj ya da programlar da dâhil olmak üzere) kasıtlı olarak değiştirmek, bozmak ya da yok etmek için gerçekleştirilen operasyonlardır (Herbert, 2010: 63).

Kritik altyapıların güvenliğinin sağlanması ve korunması açısından siber güvenliğin öneminin ortaya çıkması ve çalışmalara başlanması, yapılan saldırıların sadece askeri alanda kısıtlı kalmamasının fark edilmesiyle başlamıştır. Bir devletin, ülke topraklarının, üslerinin, ordunun veya ulusal güvenliğinin askeri alanlarla kısıtlı olmadığının anlaşılması, ülkelerin stratejik açıdan önem arz eden bölgeleri ve alanları korumaya itmiştir. Kritik altyapıların korunması da tam olarak bu noktada gündeme gelmiştir. Kritik altyapıların ülkelere zarar verilmesi konusunda önemli bir hedef olduğu düşünülmüştür. Kritik altyapılara yapılması olası saldırılar, ülkeleri savunma, ekonomi ve algı yönünden yıpratmayı amaçlamaktadır. Özellikle söz konusu olan ülkenin ulusal güvenliği hedef alınıyorsa adres kritik altyapılarından geçmektedir.

1990'yı yılların ortalarına kadar ulusal güvenlik konusundan ele alınmamış olan siber güvenlik, 1995 yılında Oklahoma'da meydana gelen bombalı saldırı sonucu önemsenmiştir (Durn Cavelty, 2008: 91). Körfez Savaşı gazisi Timothy McVeigh ve suç ortağı Terry Nichols Oklahoma City'de Alfred Murnah binasına bomba yüklenmiş bir araçla saldırı düzenlenmiştir. Saldırının sonucunda binanın üçte biri yıkılmış ve federal ofis binasında 19'u çocuk olmak üzere 168 kişi hayatını kaybetmiştir. Yaralı sayısı ise 680'dir. Bu saldırı, Pearl Harbor ve 11 Eylül saldırılarıyla beraber ABD ana toprağında gerçekleşmiş olan en ölümcül saldırılar arasında yerini almıştır (MacFarquhar, 2020).

Bu olayla birlikte daha önce de belirtildiği gibi saldırıların sadece askeri alanlarda kalmadığı acı bir şekilde fark edilmiştir. Kritik altyapılar denilen sistemlerin daima bir tehdit altında olması, özellikle de siber saldırılar ve sabotajların önlenmesi devletler açısından zorlu olduğu kadar, "caydırıcı güç" kullanması gerektiği bir alan olarak görülmeye başlanmıştır. Örneğin Pentagon başka bir ülke ya da mecradan gelecek bir siber saldırıya karşı bunun bir savaş nedeni olduğunu ve askeri güç ile karşılık verilebileceğini belirtmiştir.

Bir siber saldırı gerçekleştiğinde yapılması gereken ilk gelişme durum tespiti yapmaktır. Saldırılan bölgenin büyüklüğü, saldırıyla etkileşime giren nüfusun büyüklüğü, sebep olabileceği ekonomik ve politik sorunlar, kitle psikoloji üzerinde yaratacağı negatiflik, çevresel kayıplar ve diğer kritik altyapılara yansıması olası olan etkileri saptanmalıdır. Bu sebeple kritik altyapıların hibrit saldırılara uğrayacağı ihtimaline göre bir bilgi haritası oluşturulmalı, kritik altyapı tesislerinde offline çalışmaya elverişli ortam geliştirilmeli, yüksek seviyede bilgi güvenliği sistemleri kullanılmalı, tespit yetenekleri ve takip yetenekleri hızlandırılmalı ve geliştirilmeli, resmi kaynaklarla sistematik, hukuka bağlı ve kurallı bilgi paylaşımı yapılmalı ve tabi uluslararası işbirlikçilerle paylaşılan bilgi sınırlı tutulmalıdır (Baban, 2020: 21).

T.C. Ulaştırma ve Altyapı Bakanlığı'nın yayınladığı 2020 – 2023 Siber Güvenlik Stratejileri ve Eylem Planı Hazırlık Çalıştayı bir vizyon belgesi oluşturmuştur. Bu belgede Türkiye'nin ulusal siber güvenliğinin sağlanması asıl amaçtır. Bu belgenin "Kritik Altyapıların Korunması ve Mukavemetin Artırılması" bölümünde ilk olarak kritik altyapı tanımına yer verilirken bu sistemlerin siber saldırılara neden maruz kaldığına yönelik bir açıklama da beraberinde yapılmıştır. Bu açıklamanın devamında Türkiye'nin önceki Ulusal Siber Güvenlik Stratejileri ve Eylem Planı'na atıfta bulunularak bahsi geçen belgelerde hedeflenen çalışmalara erişildiği ve çalışmaların bu minvalde devam edeceği vurgulanmıştır.

Bu devam eden çalışmalar adına kritik altyapılar "stratejik amaç" olarak belirtilmiştir ve "*siber tehditler karşısında kamu ve özel sektörün korunmasını sağlayacak tedbirler alınarak ulusal*

mukavemetin artırılması hedeflenmektedir" denilmiştir (T.C Ulaştırma ve Altyapı Bakanlığı, 2020). Bu çalışmalarda; uluslararası alanda bilgi güvenliğinin korunması konusunda belirlenen standartların Türkiye'de de kamu ve özel sektörlerde uygulanıp yaygınlaştırılacağı, altyapılarda dışa bağımlılığın önüne geçilmesi gerektiği ve millileştirme adımının bir parçası olarak görülecek olan yurt içinde üretilen verilerin yurt içinde kalması gerektiği vurgulanmıştır.

Bilgi ve iletişim güvenliği konusunda zafiyetler günümüzde büyük önem taşımaktadır. Bu konudaki eksikliklerin belirlenmesi ve bu eksikliklerin giderilmesi adına atılacak isabetli adımlar, ülkenin ulusal siber güvenliğini sağlamak adına büyük önem arz etmektedir. *"Siber güvenlik konusu özellikle 2008 senesi itibariyle Avrupa Birliği, Ekonomik İşbirliği ve Kalkınma Teşkilatı, Kuzey Atlantik Paktı gibi uluslararası kuruluşlara ek olarak kendi devlet düzeyinin ve halkının güvenliğini sağlama almak isteyen ülkelerin de literatürüne katılmış ve gündeme alınmıştır"* (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016: 6).

Bu çerçevede, kritik altyapıların ve siber uzaydaki tüm ulusal varlıkların siber saldırılara karşı olarak etkin bir biçimde korunması ve herhangi bir siber olaya müdahale kabiliyetinin daha da güçlendirilmesi hedeflenmiştir. Ek olarak sektörel ve ulusal ölçekte bir risk yönetimi anlayışıyla tehditlerin ve oluşturdukları olumsuz etkilerin en aza indirgenmesi amaçlanmıştır (T.C Ulaştırma ve Altyapı Bakanlığı, 2020: 24).

Sonuç

Bu çalışmada öncelikle kritik altyapı kavramının tanımına yer verildi. Bu tanımın dünyadaki diğer ülkeler ya da uluslararası kuruluşlar için de farklı farklı tanımları olduğuna dikkat çekildi. Bu farklı tanımlanmanın sebebi şüphesiz ülkelerin kendi bulundukları coğrafyadan konjonktüre kadar kendi güvenlikleri ve olası tehditlerini değerlendirme şekilleri, ekonomik öncelikleri, jeostratejik konumları, politik konumları ve içinde bulundukları örgüt ya da uluslararası bir işbirliği grubunun politikası ve önceliklerine göre bu ülkelerin kendilerine yön vermesidir.

Diğer bir yönden kritik altyapıların ve tesislerin korunması amaçlı örgütsel yapı ve planlamalarda da değişiklikler söz konusudur. ABD'de bu amaca yönelik olarak Yurt Güvenliği Teşkilatı (Department of Homeland Security – DHS) kurulmuştur. Amerika Birleşik Devletleri'ndeki bütün kritik altyapı tesislerinin korunmasına yönelik DHS, "Ulusal Altyapı Koruma Planı" geliştirmiş ve bu bazda sektörlere göre kendi aralarında bir planlama hazırlamaları hedeflenmiştir.

Avrupa Birliği'nde ise katmanlı yetki ve orantısallık ilkeleri esas alınmış ve ona göre bir yapılanma kurulmuştur. Katmanlı yetki ilkesine göre, her üye kritik altyapı tesislerinin korunması konusunda kendinden sorumlu olacaktır. Avrupa Birliği'ni etkileyecek ve AB tarafından belirlenmiş tesislerin korunması ise AB tarafından sağlanacaktır. Orantısallık ilkesine göre ise bu tesislerin korunmasına yönelik harcamalarda gereğinden fazla bir kaynak kullanılması kısıtlanmış ve aynı şekilde zaman konusunda da kısıtlamaya gidilmiştir.

Türkiye'de ise bu konu ağırlıklı olarak bilgi güvenliği kapsamında ele alınmıştır ve bu işin yansımasında karşımıza AFAD ve T.C. Ulaştırma ve Altyapı Bakanlığı çıkmaktadır. Bahsi geçen kurum ve kuruluşlar tarafından bir strateji belirlenmeye çalışılmış ve yapılanmaya gidilmiştir. Bu çalışmaların ilki ise AFAD tarafından hazırlanan 2014 – 2023 Kritik Altyapıların Korunması Yol Haritası Belgesi olmuştur. Bu belgeye göre Türkiye'de kritik altyapılar ulusal bir konudan daha ziyade uluslararası bir alanda çalışılması gereken bir disiplin olarak görülmüştür.

Türkiye gibi jeopolitik ve jeostratejik açıdan önemli bir ülkede kritik altyapıların zarar görmesi ya da işlevini yitirmesi durumunda meydana gelen zarar ve aksama sadece yurt içerisinde değil, bağımlı bağlantılı olan ülkeler adına da büyük problemlere yol açabilir. Bu konuda akla gelen ilk örnek tabi petrol ve doğalgaz hatlarıdır. Bu çalışmada da petrol ve doğalgaz hatları ele alındı ve bu çerçeve içerisinde kritik altyapıların korunmasına yönelik atılan adımlar incelendi.

Çalışmanın üçüncü başlığında da belirtildiği üzere petrol ve doğalgaz gibi enerji kaynaklarının bir yerden diğer bir yere naklini sağlayan enerji nakil hatları, ulusaldan uluslararasına doğru birbiriyle bütünleşmiş durumda olan hatlardır. Bütünleşmiş olma özelliklerinden ötürü bu hatların bir noktasında problem ortaya çıkması halinde bütün sistem bu problemden etkilenmektedir. Bu problemler; sabotaj, hırsızlık, fiziki ya da siber alanda yapılan terör saldırıları vb. olarak sayılabilir.

Türkiye'de yukarıda sayılan problemlerin yaşanmaması için çalışan ve bu ihtimalleri en aza düşürmek için uğraş veren kurum ve kuruluşlar birçok güvenlik önlemi almaktadırlar. Özellikle son yıllar temel alındığı zaman bu konular savunma sanayi alanına girdiğinden ötürü, savunma sanayi şirketleri birçok sistem geliştirmekte ve altyapı güvenlik riskini en aşağıya çekmeye çalışmaktadır. Türkiye uluslararası platformda bir tür enerji köprüsü görevi görmekte ve uluslararası topraklara doğru boru hatları uzanmaktadır. Bu hatların uzunluğu ne kadar artarsa aslında var olan tehditler ve güvenliği sağlama zorluğu da o denli artmaktadır.

Türkiye adına gerek coğrafi şartlar gerekse de politik anlamda izlenen yollar gereği terörizm, en başta gelen problemlerden biridir. Terör kavramı Türkiye'de sadece ülke sınırlarını değil bu tip hayati sistemleri de vurmuştur ve tehdit etmiştir. 2015 senesinde "Türkiye – İran Doğalgaz Boru Hattı"na yapılan saldırı bunu açık bir şekilde göstermiştir. Bu saldırıların hemen 1 ay sonrasında bu sefer de Bakü – Tiflis – Erzurum Doğalgaz Boru Hattı'na yönelik bir saldırı meydana gelmişti. Bir diğer saldırı çeşidi ise siber saldırılar olmuştur.

Gerçekleşen saldırılar ile meydana gelen çevresel sıkıntılar, mali kayıplar ve tahribatlar ülke ekonomisine darbe indirip, kalkınmayı olumsuz bir şekilde etkilemektedir. Buna karşılık dışarıdan alınan enerjiye bağımlı olan Türkiye adına enerji şirketlerinin millileştirilmemesi de bir tehdit ve risk oluşturmaktadır. Bu sebeple Türkiye bilgi güvenliği ve bu sistemlerin korunması adına millileştirilme yolu izlemektedir.

Türkiye'de altyapıların güvenliğine ilişkin ABD merkezli Honeywell şirketinin öne çıktığı gözlemlenmektedir. Honeywell 1992 yılından beri Türkiye'de çeşitli sistemlerde güvenliği sağlamak ve bu sistemleri daha verimli hale getirmek için birtakım çalışmalar yapmaktadır. Türkiye bu sistemlerin korunması için Honeywell şirketinin geliştirdiği işletim sistemlerini, teknolojileri, ekipmanları ve yazılımları kullanmaktadır. Yukarıda belirtildiği üzere Türkiye dışa bağlılıktan uzaklaşmak ve millileşmek amacıyla 2016 yılında Aselsan ve Havelsan savunma şirketleri ile "Savunma Sanayii Başkanlığı ile Boru Hatları Güvenliği Projesi" sözleşmesini imzalamış ve iki şirketin ortaklığıyla beraber boru hatları için güvenlik sağlayan savunma sistemleri geliştirmeyi planlamıştır.

Bu adımların yanısıra Türkiye, kritik altyapı sistemlerinin siber saldırılara da maruz kalabileceği farkındalığı ile belirli adımlar atmıştır. T.C. Ulaştırma ve Altyapı Bakanlığı'nın yayınladığı 2020 – 2023 Siber Güvenlik Stratejileri ve Eylem Planı Hazırlık Çalıştayı bir vizyon belgesi oluşturmuştur. Bu belgede Türkiye'nin önceki Ulusal Siber Güvenlik

Stratejileri ve Eylem Planı'na atıfta bulunularak bahsi geçen belgelerde bahsedilen hedeflere erişildiği ve çalışmaların bu minvalde devam edeceği vurgulanmıştır.

Bu belge nazarında ve atılan somut adımlar ışığında Türkiye'nin konuya yaklaşıma bakıldığı zaman, millileştirme hareketi geç kalınmış olsa bile doğru bir adımdır. Geçtiğimiz günlerde BAYKAR Teknoloji şirketinin sahibi ve Türkiye'nin savunma sanayisinde önemli atılımlara yol açan Sayın Selçuk BAYRAKTAR'a yönelik sorulan Yurt dışına ihraç edilen SİHA'ların Türkiye'ye karşı kullanılıp kullanılamayacağı yönündeki soruya BAYRAKTAR şöyle cevap verdi: "Biliyorsunuz ki bunlar yüksek teknoloji cihazları ve yüksek teknoloji cihazlarını yazılımlarla donatıyorsunuz. Yazılıma da sadece o teknolojiyi geliştirenler hükmediyor."

Bu cümleden de anlaşılacağı üzere ithal edilen teknolojik her türlü yazılımda bu yazılımı ihraç eden firma ve ülkelerin hâkimiyeti söz konusudur. Bu sebeple özellikle güvenlik konusunda bir yazılımı dışarıdan ithal etmek düşüncesi ve politikası yanlış bir politika olacaktır. Türkiye uzun yıllar boyunca ABD menşeili Honeywell şirketiyle yapılan işbirliği sonucunda güvenlik ve bilgi sistemlerini ABD'ye açmıştır. Bu durum Türkiye'nin var olan güvenliğinde soru işaretleri uyandırmıştır. Son yıllarda atılan doğru adımlar ile beraber oluşturulan yerli SCADA sistemlerinin güvenliğini sağlayacak altyapıların da kuvvetlendirilmesi ve SCADA sistemlerine yönelik bilgi dağarcığı yüksek yerli insan kaynağı gerekmektedir. Özellikle 5G internet altyapısının kapıda olması ve bunun var olan ve olası saldırılarda saldırganlara da hız kazandıracak olması önemli bir noktadır. Bu süreçte Türkiye'nin de bu teknolojik altyapıdan geri kalmaması ve gelişmeleri yakinen takip edip ayak uydurması gereklidir.

Türkiye'nin hâlihazırda kurulu olan ve olası kurulacak hatlarda güvenliği sağlamadan yeni adımlar atması Türkiye adına bir felakete sebebiyet verebilir. Çalışma boyunca atılan adımlar göz önüne sürülmüş ve alınabilecek diğer önlemlerden de bahsedilmiştir. Türkiye'nin enerji konusunda öne çıkması dağıtıcı rolüyle uluslararası sermayede yerini sağlamlaştırması adına bu çalışmalar çok büyük önem arz etmektedir.

Kaynakça

AFAD (2014a). 2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi, Ankara: Başbakanlık Afet Acil Durum Yönetimi Başkanlığı.

AFAD (2014b). Açıklamalı Afet Yönetimi Terimleri Sözlüğü, Ankara: Başbakanlık Afet Acil Durum Yönetimi Başkanlığı.

Ak, T. (2019). "İç Güvenlik Yönetimi Açısından Kritik Altyapıların Korunması", Assam Uluslararası Hakemli Dergi, 13. Uluslararası Kamu Yönetimi Sempozyumu Bildirileri Özel Sayısı, ss. 42-51.

Australian National Security, Security Legislation Amendment (Critical Infrastructure Protection) Act (2022). https://www.ag.gov.au/national-security/national-security-information-act, (Erişim Tarihi: 06.01.2023).

Baban, E. (2020). "İletişim, Bilgi Tekonolojileri ve Telekomünikasyon Alanında Hizmet Veren Kurumların Korunması", Kritik Altyapı ve Tesislerin Korunması, F. Erenel ve E. Caymaz (Ed.), Ankara: Nobel Akademik Yayıncılık.

Bıçakcı, S. (2019). "Hibrit Savaş", Güvenlik Yazıları Serisi, No. 33, https://trguvenlikportali.com/wpcontent/uploads/2019/11/HibritSavas_SalihBicakci_v.1.pdf, (Erişim Tarihi: 28.03.2023).

BOTAŞ (2018). "Boru Hatlarımız Yerli Güvenlik Sistemlerine Emanet", https://www.botas.gov.tr/Icerik/boru-hatlarimiz-yerli-guvenlik/44, (Erişim Tarihi: 16.01.2023).

BOTAŞ (2023). "Ham Petrol Boru Hatları", https://www.botas.gov.tr/Sayfa/ham-petrol/13, (Erişim Tarihi: 06.01.2023).

Canada's Critical Infrastructure (2022). https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/cci-iec-en.aspx, (Erişim Tarihi: 06.01.2023).

Clinton, W. J. (1996). Executive Order 13010-Critical Infrastructure Protection, Washington DC: White House.

Collins, A. (2017). Çağdaş Güvenlik Çalışmaları, (Çev. Nasuh Uslu), İstanbul: Röle Akademik Yayıncılık.

Doğan, A. , Abacı, F. (2021). "Türkiye'de Siber Terörizme Karşı Bilişim Teknolojilerinin Kullanımı" , Uluslararası Toplum Araştırmaları Dergisi, Cilt: 18 Sayı: 42, ss. 5968-5998.

Durn Cavelty, M. (2008). Cyber – Security and Threat Politics: US Efforts to Secure the Information Age, New York: Routledge.

Erenel, F. , Caymaz, E. (2020). Kritik Altyapı ve Tesislerin Korunması, Ankara: Nobel Akademik Yayınları.

Erkal, H. Y. (2018). "Enerji Güvenliğine Yönelik Tehditler ve Enerji Güvenliği Politikalarındaki Değişim" Kırşehir Ahi Evren Üniversitesi İktisadi Ve İdari Bilimler Fakültesi Dergisi, Cilt: 2, Sayı: 2, ss. 63-78.

Erol, M. S. , Şafak, O. (2015) "Hibrit Savaş Çalışmaları ve Kırım'daki Rusya Örneği", Gazi Akademik Bakış, Cilt: 9, Sayı: 17, ss. 261-277.

EU COM702(F1) (2004). "Critical Infrastructure Protection in the Fight Against Terorism", Brussels: Communication from the Commision to the Council and the European Parliament, http://ec.europa.eu/transparency/regdoc/?fuseaction=list&coteId=1&year=2004&number=702&language=EN, (Erişim Tarihi: 06.01.2023).

Gerasimov V. (2013). "Geleceğin Bilimsel Değerleri", http://vfes.ru/vpk_08_476.pdf, (Erişim Tarihi: 28.03.2023).

Germany Federal Office for Information Security (2004). https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KRITIS/acis_paper_en_pdf.html, (Erişim Tarihi: 06.01.2023).

Gordon K. ve Dion M. (2018). "Protection Of 'Critical Infrastructure' and The Role Of Investment Policies Relating To National Security", Organisation for Economic Cooperation and Development (OECD), https://www.oecd.org/daf/inv/investment-policy/40700392.pdf, (Erişim Tarihi: 06.01.2023).

HAVELSAN (2023). "Boru Hatları Güvenliği İçin Milli Güç Birliği", https://www.havelsan.com.tr, (Erişim Tarihi: 16.01.2023).

Herbert, S. L. (2010). "Offensive Cyber Operations and the Use of Force" Journal of National Security Law & Policy, Vol: 4, No: 63, ss. 63-86.

Hoffmann, F. G. (2007). Conflict in the 21st Century: The Rise of Hybrid Wars, Arlington, Virginia: Potomac Institute for Policy Studies.

Karanacak B. (2011). "Kritik Altyapılar ve Kritik Altyapıların Korunması" , İstanbul: Siber Savunma Sempozyumu.

Macfarquhar, N. (2020). "Oklahoma City Marks 25 Years Since America's Deadliest Homegrown Attack", https://www.nytimes.com/2020/04/19/us/Timothy-McVeigh-Oklahoma-City-Bombing-Coronavirus.html, (Erişim Tarihi: 21.01.2023).

Mattis, N. J. , Hoffman, F. G. (2005). Future Warfare: The Rise of Hybrid Wars, U.S. Naval Institute, Vol: 132, No: 11.

Moteff, J. , Parfomak, P. (1988). Fragile Foundations: A Report on America's Public Works, Final Report to the President and Congress, Washington D.C.: National Council on Public Works Improvement.

Moteff, J. ve Parfomak, P. (2003). "Office of the President", The National Strategy for the Physical Production of Critical Infrastructure and Key Assets.

Netherlands National Coordinator for Counterterrorism and Security Ministry of Justice and Security (2018). https://english.nctv.nl/topics/critical-infrastructure-protection, (Erişim Tarihi: 06.01.2023).

Schmitt, M. N. (2013). Tallinn Manual on The International Law Applicable to Cyber Warfare, Cambridge: Cambridge University Press.

Şahin G. (2020). "Devlete Ait Kurumlar ve İdari Altyapı Tesislerinin Korunması", Kritik Altyapı ve Tesislerin Korunması, F. Erenel ve E. Caymaz (Ed.), Ankara: Nobel Akademik Yayıncılık.

T.C Ulaştırma ve Altyapı Bakanlığı, (2020). 2020 – 2023 Ulusal Siber Güvenlik Stratejileri ve Eylem Planı.

T.C. Enerji ve Tabii Kaynaklar Bakanlığı (2023a). "Boru Hattı ve Projeleri", https://enerji.gov.tr/neupgm-boru-hatlari-ve-projeleri, (Erişim Tarihi: 06.01.2023).

T.C. Enerji ve Tabii Kaynaklar Bakanlığı (2023b). "Boru Hattı ve Projeleri, Doğalgaz Boru Hatları", https://enerji.gov.tr/bilgi-merkezi-dogal-gaz-boru-hatlari, (Erişim Tarihi: 15.01.2023).

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, (2016). 2016 – 2019 Ulusal Siber Güvenlik Stratejisi.

Toptaş, E. (2015). ''Harbin Doğası ve Karakteri Bağlamında Hibrid Savaş'', Millî Güvenlik ve Askerî Bilimler Akademik Dergisi, Cilt: 2, Sayı: 8, ss. 1-17.

UN CTED (2017). "Protection of Critical Infrastructure against Terrorist Attacks", UN Security Council Counter Terrorism Committee Executive Directorate Trends Report.

UN CTED ve UNOCT (2018). "The Protection of Critical Infrastructure Against Terrorist Attacks: Compendium of Good Practices", Counter Terrorism Committee Executive Directorate & United Nation Office of Counter Terrorism.

UN Security Council (2001). Resolution 1373 (2001), 28 September 2001.

UN Security Council (2001). Resolution 1566 (2004), 8 October 2004.

United Kingdom Home Office Security (2012). "Counter Terrorism Strategy: Protecting the Critical National Infrastructure", https://www.gov.uk/government/organisations/defence-infrastructure-organisation, (Erişim Tarihi: 06.01.2023).

US PCCIP (1998). "Critical Foundations Protecting America's Infrastructures", The Report of the President's Commission on Critical Infrastructure Protection President's Commission on Critical Infrastructure Protection, Washington DC: White House.

Ünver, M. vd. (2011). Kritik Altyapıların Korunması, Ankara: Bilgi Teknolojileri ve İletişim Kurumu.

Yavuz, A. S. (2020). "Enerji Altyapılarının Korunmasının Artan Önemi: Doğalgaz Boru Hattı Güvenliği Üzerine Bir İnceleme", Kritik Altyapı ve Tesislerin Korunması, F. Erenel ve E. Caymaz (Ed.), Ankara: Nobel Akademik Yayıncılık.